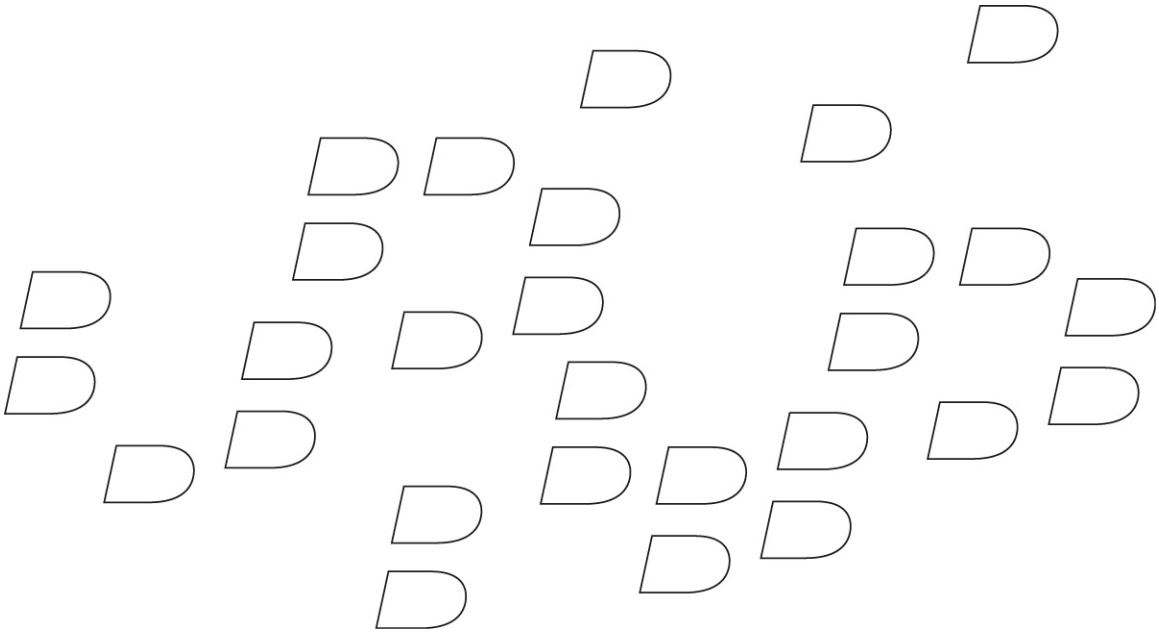


BlackBerry Smart Card Reader Security

Version 1.5

Technical Overview

Contents

This document describes the security features that the BlackBerry® Smart Card Reader Version 1.5 and the BlackBerry Enterprise Server Version 4.0.2 or later (with the correct IT policy template) support, unless otherwise stated. See the documentation for earlier software versions of the BlackBerry Smart Card Reader and the BlackBerry Enterprise Server to determine if an earlier version supports a specific feature.

See the *BlackBerry Enterprise Solution Security Acronym Glossary* for the full terms substituted by the acronyms in this document.

BlackBerry Smart Card Reader

The BlackBerry Smart Card Reader for BlackBerry devices is an accessory that, when used in proximity to certain Bluetooth® enabled BlackBerry devices and computers, integrates smart card use with the BlackBerry Enterprise Solution™, enabling users to authenticate with their smart cards to log in to Bluetooth enabled BlackBerry devices and computers.

The BlackBerry Smart Card Reader

- is designed to communicate over the wireless network with Bluetooth wireless technology version 1.1 or later–enabled BlackBerry devices and computers using the AES 256 encryption method (by default) on the application layer
- creates a reliable two-factor authentication environment for granting users access to BlackBerry and PKI applications
- is designed to enable the wireless digital signing and encryption of wireless email messages sent from the BlackBerry device using the S/MIME Support Package
- stores all encryption keys in RAM only and never writes the keys to flash memory

Authenticating a user using a smart card

The BlackBerry Smart Card Reader allows you to use two-factor authentication, using a smart card, to require users to prove their identity to the BlackBerry device or computer by two factors:

- what they have (the smart card)
- what they know (their smart card password)

Integrating a smart card with existing secure messaging technology

In addition to standard BlackBerry encryption, you can enable secure messaging technology to offer an additional layer of security between the sender and recipient of an email or PIN message. The S/MIME Support Package is designed to enable BlackBerry device users who are already sending and receiving S/MIME messages using their desktop email applications to send and receive S/MIME protected messages using their BlackBerry devices. Users can sign, encrypt, and send S/MIME messages from their BlackBerry devices. The Blackberry device can decrypt received messages that are encrypted using S/MIME to be read on the BlackBerry device.

Users might require a smart card authenticator module and must have a smart card driver and the BlackBerry Smart Card Reader driver installed on their Bluetooth enabled BlackBerry devices to perform a Bluetooth pairing followed by a secure pairing with their BlackBerry Smart Card Readers. The S/MIME Support Package supports smart card use and includes tools for obtaining certificates and transferring them to the BlackBerry device for use with the S/MIME Support Package.

After the BlackBerry device and the BlackBerry Smart Card Reader establish a secure pairing, you can set the S/MIME Force Smartcard Use IT policy rule to require the use of the smart card to sign, encrypt, or sign and encrypt S/MIME-protected messages on the BlackBerry device.

New in this release

Feature	Description
BlackBerry Smart Card Reader connections to Bluetooth enabled computers	• The BlackBerry Smart Card Reader supports connections to Bluetooth enabled computers that have the BlackBerry Smart Card Reader driver and a supported smart card driver installed. • The BlackBerry Smart Card Reader uses the same security protocols to establish a secure pairing with the computer that it uses to establish a secure pairing with the BlackBerry device. • The BlackBerry Smart Card Reader supports connections to one supported Bluetooth enabled computer and one supported Bluetooth enabled BlackBerry device at the same time. • You can set BlackBerry Enterprise Server IT policy rules in the BlackBerry Manager and use a user interface on the computer to manage BlackBerry Smart Card Reader connections to the computer.

System requirements

The BlackBerry Smart Card Reader Version 1.5 and later supports the following software and BlackBerry devices.

BlackBerry Enterprise Server	Computer	BlackBerry devices
BlackBerry Enterprise Server Version 4.0 Service Pack 2 or later for Microsoft Exchange	Microsoft® Windows® XP Service Pack 2 with support for Bluetooth technology enabled	Java™ based Bluetooth enabled BlackBerry devices that run BlackBerry Device Software Version 4.0 or later

BlackBerry Smart Card Reader upgrades

Before you can upgrade the BlackBerry Smart Card Reader, you must first reset the BlackBerry Smart Card Reader to remove the Bluetooth pairing information and the secure pairing key. See the *BlackBerry Smart Card Reader Getting Started Guide* for more information on resetting the BlackBerry Smart Card Reader. See "Appendix G: BlackBerry Smart Card Reader reset process" on page 26 for more information on the actions that the Blackberry Smart Card Reader performs when it resets.

System architecture

The BlackBerry Smart Card Reader is designed to connect to Bluetooth enabled BlackBerry devices, Bluetooth enabled computers, and PKIs. When the BlackBerry device pushes an IT policy to the BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader preserves the BlackBerry Enterprise Server signature on the IT policy. The BlackBerry Smart Card Reader cannot communicate with the BlackBerry Enterprise Server directly.

BlackBerry Enterprise Solution security

The BlackBerry Enterprise Solution (consisting of a BlackBerry device, BlackBerry Device Software, BlackBerry Desktop Software, and the BlackBerry Enterprise Server) is designed to preserve the integrity, confidentiality, and authenticity of your corporate data.

The BlackBerry Enterprise Solution is designed so that data remains encrypted (in other words, it is not decrypted) at all points between the BlackBerry device and the BlackBerry Enterprise Server. Only the BlackBerry Enterprise Server and the BlackBerry device can access the data that they send between them.

The BlackBerry Enterprise Solution uses a symmetric key encryption algorithm, which is designed to provide strong security, to protect all data that the BlackBerry device and the BlackBerry Enterprise Server send between them while the data is in transit. The BlackBerry Enterprise Solution uses either the Triple DES algorithm or the AES algorithm for this standard BlackBerry encryption, which is designed to verify that a BlackBerry message remains protected in transit to the BlackBerry Enterprise Server while the message data is outside the corporate firewall.

Bluetooth enabled BlackBerry devices

BlackBerry devices that use Bluetooth wireless technology are designed to establish a wireless connection with other Bluetooth enabled devices, such as a hands-free car kit or a wireless headset, that are within an approximate 10-meter range of these BlackBerry devices.

Bluetooth profiles specify how applications on Bluetooth enabled BlackBerry devices and on other Bluetooth devices connect, and how those applications are interoperable. The Bluetooth Serial Port Profile on Bluetooth enabled BlackBerry devices specifies how the BlackBerry device and another Bluetooth enabled device can establish a serial connection between them using a virtual serial port. Bluetooth enabled devices access the virtual serial port through the BlackBerry Software Development Kit.

Bluetooth enabled BlackBerry devices running BlackBerry Device Software Version 4.0 or later are designed to provide the following security measures by default on the Bluetooth wireless channel, which is widely considered to be non-secure:

- The Bluetooth wireless transceiver on the BlackBerry device is turned off.
- Users must request a connection between the Bluetooth enabled BlackBerry device with a Bluetooth device and type a password called a passkey, which is a shared secret key, to complete the pairing.
- Users can specify whether or not the BlackBerry device uses the passkey to encrypt data that the user sends over a Bluetooth connection.
- The Bluetooth enabled BlackBerry device prompts the user each time a Bluetooth enabled device attempts to connect to the BlackBerry device.
- The Bluetooth enabled BlackBerry device never enters into discoverable mode unless the user turns on that feature.

Managing Bluetooth enabled BlackBerry devices

Using BlackBerry Enterprise Server Software Version 4.0 or later, you can set BlackBerry Enterprise Server IT policy rules that are designed to control the behavior of Bluetooth enabled BlackBerry devices, including the following examples:

- prevent Bluetooth enabled BlackBerry devices from establishing a Bluetooth connection to another Bluetooth enabled BlackBerry device, another Bluetooth enabled device, or the BlackBerry desktop software
- prevent users from turning on discoverable mode on Bluetooth enabled BlackBerry devices
- require Bluetooth enabled BlackBerry devices to use Bluetooth encryption on all connections
- require Bluetooth enabled BlackBerry devices to prompt the user to type the BlackBerry device password to turn on Bluetooth support
- require Bluetooth enabled BlackBerry devices to prompt the user to type the BlackBerry device password to turn on discoverable mode
- prevent Bluetooth enabled BlackBerry devices from using the Bluetooth Headset Profile, the Bluetooth Handsfree Profile, or the Bluetooth Serial Port Profile
- prevent Bluetooth enabled BlackBerry devices from using wireless bypass over a Bluetooth connection
- prevent Bluetooth enabled BlackBerry devices from sending or receiving address book information over a Bluetooth connection
- prevent Bluetooth enabled BlackBerry devices from making phone calls

See the *Policy Reference Guide* for more information.

Bluetooth security measures on the BlackBerry Smart Card Reader

The following default security methods on the BlackBerry Smart Card Reader enhance the existing protection of the Bluetooth wireless technology on Bluetooth enabled BlackBerry devices.

Security method	Description
Limited use of discoverable mode	When the user starts the Bluetooth connection process between the BlackBerry Smart Card Reader and the Bluetooth enabled BlackBerry device or computer, the BlackBerry Smart Card Reader enters into discoverable mode long enough for the BlackBerry device or computer to search for the BlackBerry Smart Card Reader and pair with it. The BlackBerry Smart Card Reader is designed to enter into discoverable mode whenever it displays the reader ID and its LED is solid green.
Limited use of serial port profiles	The BlackBerry Smart Card Reader uses the Bluetooth Serial Port Profile only, allowing you to use application control to shut down all the other profiles and prevent third-party applications from using the BlackBerry Smart Card Reader.
Bluetooth pairing process helps prevent passive attack	The BlackBerry Smart card Reader Bluetooth pairing process uses a random key (unlike the hard-coded keys that headsets and other Bluetooth enabled devices use). The Bluetooth pairing process is always user-driven from the BlackBerry device or computer. If a message prompts users to type a pairing password when they did not start a pairing process, they know that another device that they might not want to connect to started the pairing process. The Bluetooth pairing process is designed to help prevent a passive attack in which an attacker attempts to search for the BlackBerry device PIN.
Control of the Bluetooth range	You can use the Maximum Bluetooth Range IT policy rule to control the Bluetooth wireless transceiver power level on the BlackBerry Smart Card Reader. Setting the power level also controls the range of proximity between the BlackBerry Smart Card Reader and the BlackBerry device at which the two parties close the Bluetooth connection between them. The range value does not translate to a specific distance because the Bluetooth range is partially determined by the power level. The range value is also heavily influenced by environmental factors, including obstructions and electromagnetic radiation. As a general rule, the Bluetooth range at power setting n+1 is longer than the range at power setting n.

BlackBerry Smart Card Reader security

The BlackBerry Smart Card Reader is designed to provide strong authentication to prevent offline and online dictionary attacks using the following security methods by default.

Security method	Description
Secure connections	The BlackBerry Smart Card Reader uses processes designed to • pair the BlackBerry Smart Card Reader with the Bluetooth enabled BlackBerry device or computer using a Bluetooth pairing key to establish a Bluetooth connection between them • pair the smart card with the Bluetooth enabled BlackBerry device or computer using a secure pairing key to establish an authenticated connection between them • establish session keys to protect data that the BlackBerry device or computer and the BlackBerry Smart Card Reader send between them on the application layer over the Bluetooth connection
Shared master encryption key	The BlackBerry Smart Card Reader creates a shared master encryption key from the secure pairing key and a secret private key that the BlackBerry Smart Card Reader sets.
BlackBerry Smart Card Reader password	The first BlackBerry device or computer to connect to the BlackBerry Smart Card Reader after the BlackBerry Smart Card Reader resets, which removes the Bluetooth pairing information, must set a connection password. This password protects the encryption keys on the BlackBerry Smart Card Reader in the same way that the BlackBerry device password protects the data on the BlackBerry device. Any debugging application that tries to connect to the BlackBerry Smart Card Reader over the USB connection cannot connect unless that application knows the password. After ten unsuccessful password attempts, the BlackBerry Smart Card Reader erases all of its data, including the password. See "Appendix G: BlackBerry Smart Card Reader reset process" on page 26 for more information.
Protected key storage	To help limit the risk of key disclosure, the BlackBerry Smart Card Reader is designed to store all keys in its RAM only and does not write keys to its flash memory. To take the BlackBerry Smart Card Reader apart, the user must remove the battery, thereby clearing all of the keys on the BlackBerry Smart Card Reader. BlackBerry devices that run the BlackBerry Device Software Version 4.1 or later and the computer store the current secure pairing key and the shared master encryption key in their respective RAM only. BlackBerry devices that run BlackBerry Device Software versions earlier than version 4.1 store the secure pairing key and the shared master encryption key in a key store database in BlackBerry device flash memory.

Security method	Description
Code signing	Before you or a user can run a permitted third-party application that uses the controlled APIs on the BlackBerry device, the Research In Motion (RIM) signing authority system must use public key cryptography to authorize and authenticate the application code. The BlackBerry Smart Card Reader uses code signing to prevent users from loading third-party code onto the BlackBerry Smart Card Reader. When RIM manufactures the BlackBerry Smart Card Reader, it installs a public key into the secure boot ROM of the BlackBerry Smart Card Reader and uses the corresponding private key to sign the BlackBerry Smart Card Reader operating systems. When RIM loads an operating system and Java Virtual Machine onto the BlackBerry Smart Card Reader, the boot ROM verifies the signature on the loaded operating system. If the boot ROM determines that the signature is not valid, it rejects the operating system. See the *BlackBerry Enterprise Solution Security Technical Overview* for more information on code signing.
Random number generation	In the BlackBerry Smart Card Reader, the following sources of entropy seed the random number generator: • RIM manufactures each BlackBerry Smart Card Reader with a random 64-byte value (a seed). This provides the BlackBerry Smart Card Reader with entropy before the wireless transceiver is turned on. • When the initial key establishment protocol establishes the master encryption key and the connection key establishment protocol establishes the connection key that the BlackBerry device or computer and the BlackBerry Smart Card Reader use to send data between them, the BlackBerry device or computer and the BlackBerry Smart Card Reader use SHA 512 to hash all of the packets that they send and receive between them and add the hashed packets to the entropy pool. • Each time the BlackBerry device or computer and the BlackBerry Smart Card Reader negotiate keys during the initial key establishment protocol and the connection key establishment protocol, the BlackBerry device or computer sends a 64-byte seed to the BlackBerry Smart Card Reader. The BlackBerry Smart Card Reader adds this value to its random source. See the *BlackBerry Enterprise Solution Security Technical Overview* for more information on the BlackBerry device random number generation process.

Managing third-party application Bluetooth connections to the BlackBerry Smart Card Reader

Application control is designed to limit the use of Bluetooth wireless technology (and the Bluetooth profiles) to specific, permitted third-party applications. Using the BlackBerry Enterprise Server Version 4.0 or later, you can set BlackBerry Enterprise Server IT policy rules and application policy rules to control how third-party applications use the BlackBerry Smart Card Reader to connect to Bluetooth enabled BlackBerry devices.

Use application control policy rules to

- permit or prevent third-party applications from being downloaded onto BlackBerry devices
- define which features (for example, the email application, the phone application, and the BlackBerry device key store) third-party applications can access on the BlackBerry device
- define the types of connections that a third-party application can establish (for example, opening network connections inside the firewall) on the BlackBerry device
- send third-party applications to BlackBerry devices over the wireless network
- prevent third-party applications that have obtained a digital signature from the RIM signing authority system from using the BlackBerry device-controlled APIs to do anything other than access persistent storage of user data and communicate with other applications

You can set application control policy rules so that all Bluetooth profiles are unavailable for applications by default and then turn on the Bluetooth Serial Port Profile for the BlackBerry Smart Card Reader driver only. In this configuration, only the necessary applications are permitted to use the BlackBerry Smart Card Reader driver.

Managing BlackBerry Smart Card Reader technology

Using the BlackBerry Enterprise Server Version 4.0 Service Pack 2 (with the S/MIME IT Policy template imported) or BlackBerry Enterprise Server Version 4.0 Service Pack 3 or later, you can set BlackBerry Enterprise Server IT policy rules that are deigned to control the behavior of the BlackBerry Smart Card Reader.

IT policy rule	Recommended use
Force Erase All Keys on BlackBerry Disconnected Timeout	Specify whether or not the secure pairing keys for the current BlackBerry device and computer connections to the BlackBerry Smart Card Reader are cleared when the BlackBerry disconnected timeout fires.
Force Smart Card Two Factor Authentication	Specify whether or not the user must type the BlackBerry device password and the smart card password to use the BlackBerry device. **Note**: Use Microsoft Windows Local Security Policy settings to specify whether or not the user must connect to a supported smart card reader from the Windows login screen to use the computer.
Force Smart Card Two Factor Challenge Response	Specify whether or not the user must choose a smart card certificate for use with smart card two-factor authentication. If smart card two-factor authentication is turned on, when the user unlocks the BlackBerry device, the BlackBerry device sends a challenge to the smart card to verify that it is the same smart card that the BlackBerry device used to initialize the authenticator module.

IT policy rule	Recommended use
Lock on Smart Card Removal	Specify whether or not the BlackBerry device locks when the user removes the smart card from a supported smart card reader or disconnects a supported smart card reader from the BlackBerry device. **Warning**: Not all smart card reader drivers support smart card removal detection. **Note**: Use Microsoft Windows Local Security Policy settings to specify whether or not a computer locks when the user removes the smart card from a supported smart card reader or disconnects a supported smart card reader from the computer.
Maximum Connection Heartbeat Period	Specify the maximum heartbeat period, in seconds. During each heartbeat period, the paired BlackBerry device or computer sends a heartbeat, which the BlackBerry Smart Card Reader acknowledges. If either side fails to send or acknowledge a heartbeat in the maximum heartbeat period, the BlackBerry device or computer closes the Bluetooth connection. **Note**: When the Bluetooth connection closes, the disconnected timer starts if you or the user enabled that feature on the BlackBerry device or computer. The BlackBerry device or computer clears the secure pairing keys when the disconnected timer expires. Use this IT policy rule to prevent an attacker from using a low-level Bluetooth heartbeat to keep the Bluetooth connection open between the BlackBerry device or computer and the BlackBerry Smart Card Reader and the secure pairing keys present, for an extended period after the BlackBerry device and BlackBerry Smart Card Reader should close the Bluetooth connection.
Maximum BlackBerry Disconnected Timeout	Specify the maximum time, in seconds, after the BlackBerry device and the BlackBerry Smart Card Reader close the Bluetooth connection between them that the disconnected timeout fires. **Note**: You can use the Force Erase All Keys on BlackBerry Disconnected Timeout IT policy rule to specify whether or not the secure pairing keys for the current BlackBerry device and computer connections to the BlackBerry Smart Card Reader are cleared when the disconnected timeout fires.
Maximum BlackBerry Long Term Timeout	Specify the maximum time, in hours, after the BlackBerry device and the BlackBerry Smart Card Reader establish the secure pairing information between them, that the BlackBerry device and the BlackBerry Smart Card Reader remove their secure pairing information.
Maximum BlackBerry Bluetooth Traffic Inactivity Timeout	Specify the maximum time, in minutes, of secure Bluetooth traffic inactivity permitted between the BlackBerry Smart Card Reader and the BlackBerry device before the secure pairing information is removed from the BlackBerry device and the BlackBerry Smart Card Reader.
Maximum Smart Card Not Present Timeout	Specify the maximum time, in seconds, after the user removes the smart card from the BlackBerry Smart Card Reader that the secure pairing information is removed from the BlackBerry device and the BlackBerry Smart Card Reader.

IT policy rule	Recommended use
Maximum Number of BlackBerry Transactions	Specify the maximum number of transactions (smart card–related operations) that the BlackBerry device and the BlackBerry Smart Card Reader can send and receive before the secure pairing information is removed from the BlackBerry device.
Maximum Bluetooth Range	Specify the maximum power range, as a value between 30% (the shortest range) and 100% (the longest range), that the BlackBerry Smart Card Reader uses to send Bluetooth packets.
Maximum PC Disconnected Timeout	Specify the maximum time, in seconds, after the computer and the BlackBerry Smart Card Reader close the Bluetooth connection between them that the secure pairing information for that dropped connection is removed from the computer and the BlackBerry Smart Card Reader.
Maximum PC Long Term Timeout	Specify the maximum time, in hours, after the computer and the BlackBerry Smart Card Reader establish the secure pairing information between them that the computer and the BlackBerry Smart Card Reader remove their secure pairing information.
Maximum PC Bluetooth Traffic Inactivity Timeout	Specify the maximum time, in minutes, of secure Bluetooth traffic inactivity permitted between the BlackBerry Smart Card Reader and the computer before the secure pairing information is removed from the computer and the BlackBerry Smart Card Reader.
Maximum Number of PC Transactions	Specify the maximum number of transactions (smart card–related operations) that the computer and the BlackBerry Smart Card Reader can send and receive between them before the secure pairing information is removed from the computer and the BlackBerry Smart Card Reader. **Note:** A transaction is any request and response set of packets other than a connection heartbeat.
Maximum Number of PC Pairings	Specify the maximum number of computers that can pair with the BlackBerry Smart Card Reader.

Note: The BlackBerry Smart Card Reader also recognizes the Disable Radio When Cradled IT policy rule, which controls whether or not the wireless transceiver is turned off when the BlackBerry device is connected to USB peripherals. If you set this IT policy rule to True, the Bluetooth wireless transceiver of the BlackBerry Smart Card Reader is turned off whenever the BlackBerry Smart Card Reader is connected to a computer using USB.

See the *Policy Reference Guide* for more information.

Establishing an encrypted and authenticated connection to the BlackBerry Smart Card Reader

Before the smart card and the BlackBerry device can establish an encrypted and authenticated connection between them, the BlackBerry Smart Card Reader and the BlackBerry device or computer must perform a Bluetooth pairing process to establish a Bluetooth connection between the BlackBerry device or computer and the BlackBerry Smart Card Reader. The BlackBerry device or computer and the BlackBerry Smart Card Reader can then perform a secure pairing process to establish a connection between the smart card and the BlackBerry device or computer that is designed to allow the BlackBerry Smart Card Reader and the BlackBerry device or computer to encrypt and authenticate the data that they send between them over the application layer.

During the secure pairing process

- the initial key establishment protocol creates a shared master encryption key on the BlackBerry device or computer and the BlackBerry Smart Card Reader that the BlackBerry device or computer and the BlackBerry Smart Card Reader use to encrypt and decrypt the data that they send between them

- the connection key establishment protocol creates a shared connection key on the BlackBerry device or computer and the BlackBerry Smart Card Reader that the BlackBerry device or computer and the BlackBerry Smart Card Reader use to send data between them

The user must perform a Bluetooth pairing once only but must perform a secure pairing each time that the BlackBerry device or computer removes the secure pairing information. You can control when the BlackBerry device or computer removes the secure pairing information using BlackBerry Enterprise Server IT policy rules for the BlackBerry Smart Card Reader.

Performing the Bluetooth pairing process and the secure pairing process on the BlackBerry device

The user can start the Bluetooth pairing process and the secure pairing process automatically by clicking Connect on the BlackBerry Smart Card Reader options screen on the BlackBerry device. If the user is running BlackBerry Device Software Version 4.0 or later on the BlackBerry device, the user can start the secure pairing process by attempting an action on the BlackBerry device that requires the smart card (for example, importing certificates, signing or decrypting a message, or turning on two-factor authentication). If the user is running BlackBerry Device Software Version 4.0.2 or later on the BlackBerry device, attempting an action on the BlackBerry device that requires the smart card can also start the Bluetooth pairing process.

See the *BlackBerry Smart Card Reader Getting Started Guide* for more information.

Performing the Bluetooth pairing process and the secure pairing process on the computer

The user must connect to the BlackBerry Smart Card Reader from the BlackBerry Smart Card Reader Options dialog on the computer manually to start the Bluetooth pairing process. When the Bluetooth pairing is established, the computer automatically prompts the user to perform the secure pairing process.

See the *BlackBerry Smart Card Reader Getting Started Guide* for more information.

Initial key establishment protocol used in the secure pairing process

The initial key establishment protocol uses the ECDH algorithm to negotiate numerous algorithms for use in subsequent secure pairing key and connection key exchanges, including the following algorithms:

- the elliptic curve used by future ECDH exchanges (The initial key establishment protocol is designed to negotiate to use 521-bit Random Curve.)
- the encryption algorithm and hash algorithms used by the encryption and authentication processes on the application layer (The initial key establishment protocol is designed to negotiate to use AES 256 and SHA 256 for application layer encryption and authentication, and SHA 512 for IT policy authentication.)

See "Appendix A: BlackBerry Smart Card Reader supported algorithms" on page 19 for more information.

Initial key establishment protocol process

1. The BlackBerry device or computer sends an initial echo of the value 0xC1F34151520CC9C2 to the BlackBerry Smart Card Reader to confirm that a Bluetooth connection to the BlackBerry Smart Card Reader exists and to verify that both sides understand the protocol.
2. The BlackBerry Smart Card Reader receives the initial echo and replies with an echo transmission of the same value.
3. The BlackBerry device or computer receives the echo.
4. The BlackBerry device or computer asks the BlackBerry Smart Card Reader for a list of supported algorithms.
5. The BlackBerry Smart Card Reader creates a list of all of the algorithms that it supports.
6. The BlackBerry Smart Card Reader sends the supported algorithms list to the BlackBerry device or computer.

7. The BlackBerry device or computer processes the list to search for a match with one of its own supported algorithms.
   - If a match is not available, the BlackBerry device or computer sends an error to the BlackBerry Smart Card Reader and stops processing the list.
   - If a match exists, the BlackBerry device or computer begins the key establishment by sending a pairing request using the selected algorithms and a 64-byte seed to the BlackBerry Smart Card Reader.
8. The BlackBerry Smart Card Reader verifies the selected algorithms.
9. The BlackBerry Smart Card Reader performs the following calculation to select a short-term key (*Y*):
   - selects random $y, 1 < y < r - 1$
   - calculates $Y = yS$
10. The BlackBerry Smart Card Reader sends *Y* to the BlackBerry device or computer.
11. The BlackBerry device or computer performs the following calculations to select a short-term key (*X*):
   - selects random $x, 1 < x < r - 1$
   - calculates $X = xS$
   - calculates the master encryption key (*MK*) using the following information:

Parameter	Value
K	$xY = xyS$
H1	SHA 512 (sent packets)
H2	SHA 512 (received packets)

   - calculates $H = H1 + H2$
   - calculates $MK = \text{SHA 256}(H \| K)$
12. The BlackBerry device sends *X* to the BlackBerry Smart Card Reader.
13. The BlackBerry Smart Card Reader calculates *MK* using the following information:

Parameter	Value
K	$yX = yxS$
H1	SHA 512 (sent packets)
H2	SHA 512 (received packets)
H	$H1 + H2$
MK	$\text{SHA 256} (H \| K)$

14. The initial key establishment protocol completes; the BlackBerry device or computer and the BlackBerry Smart Card Reader share a master encryption key.

See "Appendix D: BlackBerry Smart Card Reader shared cryptosystem parameters" on page 22 for more information on variables used in this process.

Connection key establishment protocol used in the secure pairing process

After the initial key establishment protocol completes successfully, the BlackBerry device or computer and the BlackBerry Smart Card Reader share a master encryption key. They must then establish a connection key to use to send data between them. The connection key establishment protocol uses SPEKE to bootstrap from the secure pairing key *s*, enabling a BlackBerry device or computer to establish long-term public keys and a strong, cryptographically protected connection with a BlackBerry Smart Card Reader.

The connection key establishment protocol uses the ECDH (elliptic curve) algorithm that the initial key establishment protocol negotiates. The ECDH algorithm provides perfect forward secrecy, which uses the key that protects data to prevent the protocol from deriving previous or subsequent encryption keys. Each run of the

connection key establishment protocol uses a unique, random, ephemeral key pair to create the new connection key. The BlackBerry Smart Card Reader discards the ephemeral key pair after establishing the connection key. Even if the ephemeral private keys from a particular protocol run using the ECDH algorithm are compromised, the connection keys from other runs of the same protocol remain uncompromised.

Connection key establishment protocol process

1. The BlackBerry device or computer sends an initial echo of the value 0xC1F34151520CC9C2 to the BlackBerry Smart Card Reader to confirm that a Bluetooth connection to the BlackBerry Smart Card Reader exists and to verify that both sides understand the protocol.
2. The BlackBerry Smart Card Reader receives the initial echo and replies with an echo transmission of the same value.
3. The BlackBerry device or computer receives the echo.
4. The BlackBerry device or computer uses the algorithm that the initial key establishment protocol negotiated to send the selected algorithms and a seed to the BlackBerry Smart Card Reader.
5. The BlackBerry Smart Card Reader performs the following calculation to select a short-term key (*Y*):

   - selects random $y, 1 < y < r - 1$
   - calculates $Y = yP$

   where *P* is defined on the curve negotiated by the initial key establishment protocol
6. The BlackBerry Smart Card Reader sends *Y* to the BlackBerry device or computer.
7. The BlackBerry device or computer performs the following calculation to select a short-term key (*X*):

   - selects random $x, 1 < x < r - 1$
   - calculates $X = xP$
   - calculates the connection key (*CK*) using the following information:

Parameter	Value
K	$xY = xyP$
H1	SHA 512 (sent packets)
H2	SHA 512 (received packets)
H	*H1* + *H2*
CK	SHA 256 ($MK \| H \| MK \| K$)

8. The BlackBerry device or computer sends *X* to the BlackBerry Smart Card Reader.
9. The BlackBerry device or computer performs a hashing function to calculate *CK*.
10. The BlackBerry Smart Card Reader calculates *CK* using the following information:

Parameter	Value
K	$xY = xyP$
H1	SHA 512(sent packets)
H2	SHA 512(received packets)
H	*H1* + *H2*
CK	SHA 256($MK \| H \| MK \| K$)

11. The connection key establishment protocol completes; the BlackBerry device or computer and the BlackBerry Smart Card Reader share a connection key.

See "Appendix D: BlackBerry Smart Card Reader shared cryptosystem parameters" on page 22 for more information on variables used in this process.

The connection key establishment protocol can stop at any point if an error occurs. See "Appendix B: Connection key establishment protocol errors" on page 20 for more information.

Encrypting and authenticating data on the application layer

When the BlackBerry device or computer and the BlackBerry Smart Card Reader complete the secure pairing process, all data that they send between them is encrypted and authenticated on the application layer by keys that they derive from the shared connection key. See "Appendix C: Application layer protocol encryption and authentication" on page 21 for more information.

The BlackBerry device or computer and the BlackBerry Smart Card Reader use AES 256 in CBC mode to encrypt the data and keyed HMAC with SHA 512 to protect data by default, but they can negotiate different algorithms during the initial key establishment protocol.

The keys protect the data on the application layer throughout the entire connection. A lost or closed connection occurs if either the BlackBerry device or the BlackBerry Smart Card Reader goes outside of a sufficient wireless coverage area or if the BlackBerry device wireless transceiver or the computer's Bluetooth transceiver turns off for any reason. When a Bluetooth connection closes, if the BlackBerry device or computer's Bluetooth connection to the BlackBerry Smart Card Reader is lost, the parties must renegotiate the keys.

You can set the Maximum Connection Heartbeat Period IT policy rule to control when the Bluetooth connection closes based on the secure heartbeat settings. See "Managing BlackBerry Smart Card Reader technology" on page 10 for more information on setting this IT policy rule.

Using two-factor authentication

If a user has a smart card authenticator module, smart card driver, and smart card reader driver installed on their BlackBerry device or computer, either you or that user can start the two-factor authentication process on the BlackBerry device or computer to bind the BlackBerry device or computer to the installed smart card. After the BlackBerry device or computer binds to the smart card, it requires that smart card to authenticate the user.

Turning on two-factor authentication on the BlackBerry device

You can set the Force Smart Card Two-Factor Authentication IT policy rule in the BlackBerry Manager to require that a user authenticates with the BlackBerry device using a smart card. If you do not force the user to authenticate with the BlackBerry device using a smart card, the user can turn two-factor authentication on and off with their smart card by setting the User Authenticator field in the BlackBerry device Security Options.

When you turn on two-factor authentication on the BlackBerry device, the following events occur:

1. The BlackBerry device locks.
2. The BlackBerry device pushes the current IT policy to the BlackBerry Smart Card Reader.
3. When a user tries to unlock the BlackBerry device, the BlackBerry device prompts the user to type the BlackBerry device password. If the user has not yet set a BlackBerry device password, the BlackBerry device forces the user to set a password.
4. The BlackBerry device prompts the user to type the user authenticator password (the smart card PIN) to turn on two-factor authentication with the installed smart card.
5. The BlackBerry device binds to the installed smart card automatically by storing the smart card binding information in a BlackBerry device NV store location that is designed to be inaccessible to the user.

When a user turns on two-factor authentication on the BlackBerry device, the following events occur:

1. The BlackBerry device prompts the user to type the BlackBerry device password. If the user has not yet set a BlackBerry device password, the BlackBerry device forces the user to set a password.
2. The BlackBerry device prompts the user to type the user authenticator password (the smart card PIN) to turn on two-factor authentication with the installed smart card.

3. The BlackBerry device binds to the installed smart card automatically by storing the smart card binding information in a BlackBerry device NV store location that is designed to be inaccessible to the user.

See "Appendix F: Smart card binding information" on page 25 for more information.

Confirming that the BlackBerry device is bound to the correct smart card

After a user turns on two-factor authentication, whenever the BlackBerry device prompts the user to insert the smart card into the BlackBerry Smart Card Reader, the BlackBerry device prompt indicates the label and the card type of the correct (bound) smart card.

The user can also view smart card information in the BlackBerry device Security Options.

Field	Description
Name	indicates the type of the installed smart card
Initialized	indicates whether or not the BlackBerry device is authenticated with and bound to the smart card • a value of Yes indicates that the BlackBerry device is bound to the smart card • a value of No indicates that the BlackBerry device is not bound to the smart card

Unbinding the smart card from the BlackBerry device

When you or the user start a BlackBerry device wipe, causing the BlackBerry device to erase its stored user and application data, the BlackBerry device removes the smart card binding information from the NV store so that a user can authenticate with the BlackBerry device using a new smart card.

You can remove the smart card binding information from the BlackBerry device manually in the following ways.

- Send the Erase Data and Disable Device IT Admin command to the BlackBerry device to remove the binding between a user's current smart card and the BlackBerry device.
- When the user turns off two-factor authentication, the BlackBerry device turns off two-factor authentication with the installed smart card and removes the smart card binding information from the BlackBerry device.

Note: If the user needs to remove smart card binding information from a BlackBerry device that is bound to a smart card using a smart card reader other then the BlackBerry Smart Card Reader, use the Smart Card Migration Tool to remove the binding between the user's current smart card and the BlackBerry device. Visit www.blackberry.com/knowledgecenterpublic/ to view the article KB-03125 "How to Download and use the Smart Card Migration Tool."

Setting two-factor authentication on the computer

See the Microsoft Windows documentation for information on configuring a computer to require the user to connect to a supported smart card reader from the Windows login screen to use the computer.

Related resources

Resource	Information
BlackBerry Enterprise Solution Security Technical Overview	• preventing the decryption of information at an intermediate point between the BlackBerry device and the BlackBerry Enterprise Server or organization LAN • managing security settings for all BlackBerry devices • protecting data in transit between the BlackBerry device and the BlackBerry Enterprise Server • understanding the algorithms provided by the RIM cryptographic application programming interface (Crypto API) • understanding the TLS and WTLS standards that the RIM Crypto API currently supports • understanding the memory scrub process that occurs on the BlackBerry device when content protection is enabled
BlackBerry Enterprise Server System Administration Guide	• generating and changing master encryption keys • enabling S/MIME • enabling encryption options • setting IT policy rules • setting message classifications
BlackBerry Smart Card Reader Getting Started Guide	• setting up the BlackBerry Smart Card Reader • installing or upgrading the BlackBerry Smart Card Reader • pairing the BlackBerry device or the computer with the BlackBerry Smart Card Reader • troubleshooting
Policy Reference Guide	• using BlackBerry Enterprise Server IT policies
S/MIME Support Package User Guide Supplement	• installing the S/MIME Support Package • managing certificates on the BlackBerry device and desktop computer • setting S/MIME options for digitally signing and encrypting messages • sending and receiving S/MIME protected messages
Security for BlackBerry devices with Bluetooth Wireless Technology	• understanding Bluetooth wireless technology • understanding the risks of using Bluetooth wireless technology on mobile devices • protecting Bluetooth enabled BlackBerry devices
Visit www.blackberry.com/security.	• information about BlackBerry Solution security

Appendix A: BlackBerry Smart Card Reader supported algorithms

Algorithm type	Algorithm
elliptic curve (default)	• 571-bit Koblitz Curve (EC571K1) • 521-bit Random Curve (EC521R1)* • 283-bit Koblitz Curve (EC283K1) • 256-bit Random Curve (EC256R1) • 160-bit Random Curve (EC160R1)
encryption	• AES 256* • AES 128
hash	• SHA 512* • SHA 256* • SHA 1

*The initial key establishment protocol is designed to negotiate to use the algorithm indicated unless the BlackBerry device or the computer requires a different, supported algorithm.

Appendix B: Connection key establishment protocol errors

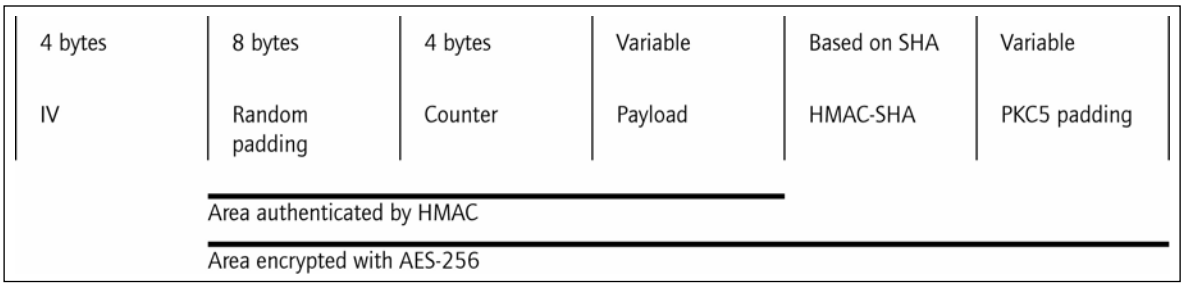
During the connection key establishment protocol process, if an error occurs on the BlackBerry device, the computer, or the BlackBerry Smart Card Reader, that party sends an error code to the other party negotiating the connection key. The following errors might occur:

- negative length
- bad packet
- incomplete crypto specification
- bad public key
- no algorithms in common are permitted
- not paired
- not connected
- connection error
- decryption error

Appendix C: Application layer protocol encryption and authentication

By default, each packet that the BlackBerry device or computer and the BlackBerry Smart Card Reader send between them is authenticated and encrypted using the following methods:

- authenticated with HMAC using the negotiated SHA algorithm
- encrypted with AES of the negotiated key size using CBC mode



Anatomy of an application layer protocol formatted packet

The connection key protocol establishes a shared connection key *CK* from which the BlackBerry device or computer and the BlackBerry Smart Card Reader derive the four session keys that they use on the application layer to protect the data that they send between them.

Connection session key	Value	Description
KeySendEnc	SHA 256(*CK* || *S1*)	the AES 256 key that the BlackBerry device, the computer, or the BlackBerry Smart Card Reader generates to encrypt the data that it sends to the other party over the application layer
KeyRecEnc	SHA 256(*CK* || *S2*)	the AES 256 key that the BlackBerry device, the computer, or the BlackBerry Smart Card Reader generates to decrypt the data that it receives from the other party over the application layer
KeySendAuth	SHA 256(*CK* || *S3*)	the HMAC authentication key that the BlackBerry device, the computer, or the BlackBerry Smart Card Reader generates to authenticate the data that it sends to the other party over the application layer
KeyRecAuth	SHA 256(*CK* || *S4*)	the HMAC authentication key that the BlackBerry device, the computer, or the BlackBerry Smart Card Reader generates to authenticate the data that it receives from the other party over the application layer

Note: *S1*, *S2*, *S3*, and *S4* are hard-coded strings that the BlackBerry device or computer and the BlackBerry Smart Card Reader use in the key derivation to prevent calculating session keys that are the same as each other.

Appendix D: BlackBerry Smart Card Reader shared cryptosystem parameters

The BlackBerry Smart Card Reader and the BlackBerry device or computer with the BlackBerry Smart Card Reader software and drivers installed are designed to share the following cryptosystem parameters.

Parameter	Description
E(Fq)	• the NIST-approved 521-bit random elliptic curve over Fq, which has a cofactor of 1 **Note:** The initial establishment key protocol does all math operations in the group E(Fq).
Fq	a finite field of prime order q
P	a point of E that generates a subgroup of E(Fq) of prime order r
xR	• a representation of elliptic curve scalar multiplication, where *x* is the scalar and *R* is a point on E(Fq).
s	• the secure pairing key value that appears on the BlackBerry Smart Card Reader display **Note**: The secure pairing key must be known only to the authorized user of the BlackBerry device or computer and the BlackBerry Smart Card Reader until the protocol completes.
S	• the secure pairing value (*s*) converted to a point on E(Fq)

Appendix E: Examples of attacks that the BlackBerry Smart Card Reader security protocols are designed to prevent

Eavesdropping

An eavesdropping event occurs when the attacker listens to the communication between the BlackBerry Smart Card Reader and the BlackBerry device or computer. The goal of the attacker is to determine the shared master encryption key on the BlackBerry Smart Card Reader and the BlackBerry device or computer, given only *xS* and *yS*.

The initial key establishment protocol and the connection key establishment protocol are designed so that the attacker can only compute the master encryption key by solving the ECDH problem. This calculation is equivalent to solving the DH problem, which is computationally infeasible.

Impersonating a BlackBerry device or computer

An impersonation of the BlackBerry Smart Card Reader occurs when the attacker sends messages to the BlackBerry device or computer so that the BlackBerry device or computer believes it is communicating with the BlackBerry Smart Card Reader. The attacker must send $X = xP$, instead of *xS* to the BlackBerry Smart Card Reader. An attacker might attempt this because the attacker does not know the secure pairing key.

The initial key establishment protocol is designed so that the BlackBerry Smart Card Reader calculates $K = yX = yxP$. To calculate the same key, the attacker must determine *y* from *Y*. This problem is considered to be computationally infeasible.

The connection key establishment protocol is designed so that

- the attacker can only guess the secure pairing key
- the attacker can only compute the master encryption key by solving the discrete log problem, which is computationally infeasible, to try to determine the secret private key on the BlackBerry device or computer

Impersonating a BlackBerry Smart Card Reader

An impersonation of the BlackBerry Smart Card Reader occurs when the attacker sends messages to the BlackBerry device or computer so that the BlackBerry device or computer believes it is communicating with the BlackBerry Smart Card Reader.

The connection key establishment protocol is designed so that

- the attacker can only guess the secure pairing key
- the attacker can only compute the master encryption key by solving the discrete log problem, which is computationally infeasible, to try to determine the secret private key on the BlackBerry device or computer

Man-in-the-middle attack

A man-in-the-middle attack occurs when the attacker intercepts and modifies messages in transit between the BlackBerry Smart Card Reader and the BlackBerry device or computer. A successful man-in-the-middle attack results in each party not knowing that the attacker is sitting between them monitoring and changing traffic.

The attacker must remain in the middle (between the BlackBerry device or computer and the BlackBerry Smart Card Reader) forever, not just for the duration of the key establishment protocol, for a man-in-the-middle attack to occur. For an attacker to successfully start a man-in-the-middle attack, the attacker must know the secure pairing key.

The initial key establishment protocol is designed to use ECDH and the shared master encryption key to prevent a man-in-the-middle attack. If an attacker learns the secure pairing key

- after the initial key establishment protocol is complete, the mathematical hardness of the discrete log problem protects the master encryption key. To determine the master encryption key, an attacker must determine one of *x* or *y*.
- before the initial key establishment protocol begins and passively watches the protocol cannot gain knowledge of the master encryption key. The secure pairing key must remain secret until the initial key establishment protocol completes successfully.

The connection key establishment protocol is designed to use SPEKE to prevent a man-in-the-middle attack through the use of the secure pairing key.

Offline attack

An offline attack occurs when the attacker attempts to send $X = xP$, instead of xS to the BlackBerry Smart Card Reader. An attacker might attempt this because the attacker does not know the secure pairing key. The initial key establishment protocol is designed so that the BlackBerry Smart Card Reader replies with $Y=xS$ and calculates $K = yX = yxP$. Meanwhile, the attacker must calculates $K = xY = yxS = yxzP$, for some z such that $S = zP$. To calculate yxP from $yzxP$ without knowledge of z corresponds to solving the discrete logarithm problem, which is computationally infeasible, for S.

Offline dictionary attack

An offline dictionary attack occurs when the attacker attempts all possible passwords and determines the correct password. The connection key establishment protocol is designed to use SPEKE to prevent a known offline dictionary attack through the use of a password (the secure pairing key) in case the attacker uses computational resources (where, in theory, nothing limits the speed at which the attacker can force the password) to determine the password.

Online dictionary attack

An online dictionary attack is similar to an offline dictionary attack, but the attacker must rely on the BlackBerry device, the computer, or the BlackBerry Smart Card Reader to determine if a key is the correct secure pairing key.

The BlackBerry Smart Card Reader supports only one attempt to guess the secure pairing key. If the guess is incorrect, the BlackBerry Smart Card Reader changes the secure pairing key before the next attempt occurs.

Small subgroup attack

A small subgroup attack occurs when the attacker attempts to limit the protocol to generate master encryption keys from only a small subset of keys.

The BlackBerry Smart Card Reader security protocols are designed to use ECDH operations that use the cofactor in their calculations and verify that the result is not the point at infinity. For example, if the attacker chooses X as the point at infinity, then K is the point at infinity regardless of what the BlackBerry Smart Card Reader chose for Y. By checking that X is not at the point of infinity, 1, or –1, the BlackBerry Smart Card Reader security protocols avert this threat.

Appendix F: Smart card binding information

When you or a user turns on two-factor authentication on the BlackBerry device, the BlackBerry device binds to the installed smart card automatically by storing the following smart card binding information in a special BlackBerry device NV store location that is inaccessible to a user.

- the name of a Java class that the BlackBerry Smart Card Reader requires
- the binding information format

  Note: In BlackBerry Device Software Version 4.2 and earlier, where the BlackBerry device does not use a challenge/response certificate, the format is a version byte with a value of 0. In BlackBerry Device Software Version 4.2, where the BlackBerry device does not use a challenge/response certificate, the format is a version byte with a value of 1.
- the smart card type

  Note: For the Common Access Card, this string is "GSA CAC".
- the name of a Java class that the smart card code requires
- a unique 64-bit identifier that the smart card provides
- a smart card label that the smart card provides (for example, "GRAHAM.JOHN.1234567890")

Appendix G: BlackBerry Smart Card Reader reset process

When a user resets a BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader performs the following actions:

- backs up the Bluetooth pairing key for the currently connected BlackBerry device, if applicable

  Note: After the user resets the BlackBerry Smart Card Reader, a BlackBerry device can perform the Bluetooth pairing process and the secure paring process to connect to the BlackBerry Smart Card Reader again. If that BlackBerry device was the last BlackBerry device to connect to the BlackBerry Smart Card Reader before the user reset the BlackBerry Smart Card Reader, the BlackBerry Smart Card Reader restores the backed up Bluetooth pairing key for that Bluetooth connection and opens the Bluetooth connection to the BlackBerry device automatically.

- removes all Bluetooth pairing information
- removes all secure pairing information
- removes all user settings
- removes the connection password
- unbinds the IT policy from the BlackBerry Smart Card Reader

  Note: The BlackBerry Smart Card Reader unbinds the IT policy by deleting the IT policy public key from its NV store so that it can receive a new IT policy and digitally signed IT policy public key from a BlackBerry Enterprise Server. The BlackBerry Smart Card Reader does not delete its stored IT policy.

Part number: 9027650 Version 4